(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－190947
（P2002－190947A）
(43)公開日　平成14年７月５日(2002.7.5)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｎ　1/387		Ｈ０４Ｎ　1/387		２Ｃ０６１
Ｂ４１Ｊ　5/30		Ｂ４１Ｊ　5/30	Ｚ	２Ｃ０８７
29/00		29/38	Ｚ	５Ｂ０２１
29/38		Ｇ０６Ｆ　3/12	Ｋ	５Ｂ０５７
Ｇ０６Ｆ　3/12		Ｇ０６Ｔ　1/00	５００Ｂ	５Ｃ０７６

審査請求　未請求　請求項の数１　ＯＬ　（全 14 頁）　最終頁に続く

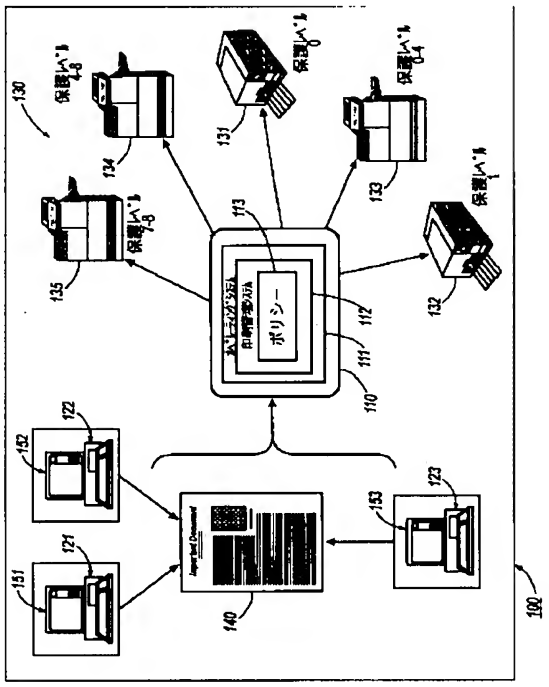
(21)出願番号　特願2001－290056(P2001－290056)
(22)出願日　平成13年９月21日(2001.9.21)
(31)優先権主張番号　０９／７２２，３６２
(32)優先日　平成12年11月28日(2000.11.28)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０９／７２２，５０８
(32)優先日　平成12年11月28日(2000.11.28)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　590000798
ゼロックス・コーポレーション
アメリカ合衆国、コネチカット州、スタンフォード、ロング・リッジ・ロード　800
(72)発明者　テレサ　エフ　ルント
アメリカ合衆国　カリフォルニア州　パロ　アルト　ブルース　ドライブ　892
(72)発明者　マチュー　ケー　フランクリン
アメリカ合衆国　カリフォルニア州　パロ　アルト　グラント　アベニュー　334
(74)代理人　100075258
弁理士　吉田　研二　（外２名）

最終頁に続く

(54)【発明の名称】　文書偽造を防止する印刷方法

(57)【要約】
【課題】　印刷される文書に応じて適切に文書偽造が防止される印刷方法を提供する。
【解決手段】　印刷される文書の価値、当該文書に対する偽造の潜在的可能性、及び偽造防止のためのコスト等を考慮して、複数の保護レベルから、当該文書に適用すべき保護レベルを判定する。判定された保護レベルに対応した透かしを印刷できるプリンタが選択され、当該プリンタを用いて当該文書の各ページが印刷される。透かしには、保護レベルに応じて、コピーの証拠を生じる仕組みや追跡情報が組み込まれる。



1

【特許請求の範囲】

【請求項１】　文書偽造を防止する印刷方法であって、少なくとも１ページを含む文書の画像を処理すること、偽造に対し前記文書に適用すべき保護レベルを判定すること、および判定された前記保護レベルに基づいて、当該保護レベルに対応するコピーの証拠および追跡情報を含む少なくとも１つの透かしを、前記文書の各ページ上に印刷すること、

を含むことを特徴とする方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、文書偽造を防止する印刷方法に関する。

【０００２】

【従来の技術】オリジナル印刷文書の偽造を検出し、かつ／または抑止する様々な技法が知られている。文書偽造は、オリジナル文書の許可されていない変更とオリジナル文書の許可されていないコピーの両方を含む。従来、偽造を検出し、かつ／または抑止するために文書に透かしが適用されている。透かしとは、文書上に印刷されたマークであって、視覚的に検知可能か、あるいは特殊な機器を使用して検出可能なものである。脆弱な透かし(fragile watermark)とは、オリジナル印刷文書に現れるが、標準的な複写機上で作成されたオリジナル文書のコピーには現れず、あるいは結果として得られる文書のコピーにおいて見て分かるほど劣化するマークである。

【０００３】頑強な透かし(robust watermark)とは、オリジナル文書に含まれる透かしが標準的な複写機上で作成されたオリジナル文書のコピーに正確に再現され、透かしに含まれる情報が当該コピーからも抽出できるものである。使用できる２種類の頑強な透かしがある。第１の種類の頑強な透かしは、オリジナル文書及びコピーの両方に現れるものである。第２の種類の頑強な透かしは、オリジナル文書上に存在するが、容易には見えず、オリジナル文書のコピー上で明確に見えるようになるものである。第２の種類の頑強な透かしは不可視頑強透かしとしても知られている。

【０００４】オリジナル文書をコピーすることによって脆弱な透かしを含むオリジナル文書を偽造することは、オリジナル文書上に透かしが存在しないことによって容易に検出される。第１の種類の頑強な透かしを含むオリジナル文書の偽造は、強いマークに含まれる情報を抽出することによって検出される。この情報は、オリジナル文書の管理者と、コピーの制限またはオリジナル文書中の情報の使用についてのその他の制限に関する情報とを与える。第２の種類の頑強な透かしを含むオリジナル文書の偽造は、オリジナル文書のコピー上に透かしが視覚的に存在することによって検出される。たとえば、第２の種類の頑強な透かしに含まれる情報は、「これはコピーです」または同様な警告を示すバナーであってよい。

2

【０００５】

【発明が解決しようとする課題】本発明は、オリジナル文書が印刷されるときにオリジナル文書に脆弱な透かしおよび頑強な透かしを付加するシステムおよび方法を提供する。

【０００６】また、本発明は、いくつかの信頼できるプリンタを使用して、偽造防止が必要な文書を印刷するシステムおよび方法を提供する。

【０００７】また、本発明は、印刷すべき文書に様々なレベルの偽造防止を行うことができるようにする一連の信頼できるプリンタを提供する。

【０００８】

【課題を解決するための手段】本発明によるシステムおよび方法の様々な例示的な実施態様によれば、一群の信頼できるプリンタが、ある範囲の様々な偽造検出および抑止技法を行うように管理される。印刷すべきオリジナル文書の保護要件は、信頼できる印刷ポリシーによって決定される。オリジナル文書に必要な保護要件を決定するために使用される要因には、作成中の文書の価値、潜在的な偽造者などが利用できる資源に関する仮定、印刷すべきオリジナル文書を保護するためのコストが含まれる。

【０００９】偽造防止が必要なオリジナル文書を印刷する際、その文書の印刷ジョブは、コピーの証拠、および／または必要なレベルの保護を得るのに必要な追跡情報を含む透かしを印刷できる信頼できるプリンタに経路指定される。コピーの証拠とは、特定の文書がオリジナル文書の許可されていないコピーであるかどうかを示す文書の検査によって得ることのできる証拠である。追跡情報とは、オリジナル文書の管理者と、管理者およびオリジナル文書に適用されるさらなるコピーに対する制限とを見極める、文書上に印刷される情報である。オリジナルをより一意に識別する働きをする他の情報を追跡情報に含めることもできる。コピーの必要な証拠は、脆弱な透かしまたは頑強な透かしを使用することによって、印刷された文書に適用される。必要な追跡情報は、頑強な透かしを使用することによって、印刷された文書に適用される。選択された信頼できるプリンタのパラメータは、透かしを印刷する印刷管理システムによって設定され、必要なレベルの保護を得るのに適切なコピーの証拠および／または追跡情報を含む。

【００１０】本発明のこれらおよびその他の特徴は、本発明によるシステムおよび方法の様々な例示的な実施形態の以下の詳細な説明に記載されており、あるいは該説明から明らかになろう。

【００１１】

【発明の実施の形態】本発明によるシステムおよび方法の様々な例示的な実施形態について以下の図面を参照して説明する。

【００１２】図１は、ポリシーベースの印刷用のシステムを示す概略図である。ネットワーク１００は、複数のコンピュータ１２１、１２２、および１２３を制御する少なくとも１つのサーバ１１０を含む。サーバ１１０は、信頼できるプリンタ１３１～１３５のファミリ１３０も制御する。信頼できるプリンタとは、ネットワーク１００の許可されたユーザのみが利用できるプリンタである。サーバ１１０は、ネットワークのユーザが、コンピュータ１２１、１２２、および１２３上のサーバ１１０に記憶されている様々なアプリケーションを使用できるようにするオペレーティングシステム１１１を含む。これらのアプリケーションには、たとえば、文書処理アプリケーション、スプレッドシートアプリケーション、画像走査アプリケーションおよび／または画像処理アプリケーション、ならびに／またはデータベース管理アプリケーションを含めることができる。コンピュータ１２１、１２２、および１２３の許可されたユーザは、サーバ１１０に記憶されており文書１４０を作成するようにオペレーティングシステム１１１によって制御されるアプリケーションを使用することができる。アプリケーションは、それぞれのコンピュータ１２１、１２２、および１２３の表示ユニット１５１、１５２、および１５３上に表示することのできる文書１４０の画像を処理する。

【００１３】文書１４０は、１つのコンピュータ１２１または１２２または１２３に印刷コマンドを入力し、サーバ１１０に印刷ジョブを送信することによって印刷することができる。オペレーティングシステム１１１は、信頼できるプリンタ１３１～１３５のファミリ１３０のうちの、印刷すべき文書１４０に必要レベルの保護を与えることのできるプリンタを選択する印刷管理システム１１２を含む。印刷管理システム１１２は、信頼できるプリンタ１３１～１３５のファミリ１３０から得られる特定のセキュリティ保護技法に文書保護要件をマップするポリシー１１３を含む。

【００１４】ポリシー１１３は、文書作成者または文書１４０の印刷を許可された他の人から文書１４０の価値に関する情報を収集することによって、印刷すべき文書１４０の必要な保護レベルを判定する。この情報には、潜在的な偽造に関する仮定と、偽造を検出しかつ／または抑止するための保護レベルを実現するのに必要なコストとを含めることができる。ユーザは、文書１４０の印刷に使用されている特定のコンピュータ１２１～１２３の表示ユニット１５１～１５３のうちの１つに設けられたグラフィカルユーザインタフェースによって文書１４０に関する情報を入力することができる。

【００１５】印刷管理システム１１２は、ユーザが、信頼できるプリンタ１３１～１３５のそれぞれに、信頼できる各プリンタ１３１～１３５がどんな保護レベルを実現するかを問い合わせることを可能にすることができる。印刷管理システム１１２は、各保護レベルでどの偽造技法を検出しかつ／または抑止することができるかと、各保護レベルの使用コストに関する情報をユーザに与えることもできる。各コンピュータ１２１～１２３は、印刷すべき文書１４０に適用できる保護レベルをユーザ表示するように印刷管理システム１１２および／またはオペレーティングシステム１１１によって制御することができる。

【００１６】印刷すべき各文書１４０には、潜在的な偽造を検出しかつ／または抑止するのに必要な保護技法の特定の組合せを識別するために印刷管理システム１１２によって使用できるセキュリティレベルが埋め込まれるか、付加されているか、あるいはその他の方法で関連付けられている。ポリシー１１３は、プログラム可能であり、ネットワーク１００を所有または使用する組織の特定の要件に適合させることができる。ポリシー１１３は、ネットワーク１００のあらゆる許可されたユーザまたはネットワーク１００のあらゆるコンピュータ１２１～１２３に保護レベルを割り当てるようにプログラムすることができる。

【００１７】ネットワーク１００のあらゆるユーザは、ポリシー１１３にプログラムされたＩＤを有することができる。このＩＤは、ログインパスワードまたはユーザＩＤであってよい。このＩＤによって識別されるユーザによって印刷されたあらゆる文書１４０に、指定された保護レベル、最小保護レベル、および／または最大保護レベルを割り当てることができる。

【００１８】ネットワーク１００のあらゆるコンピュータ１２１～１２３はＩＤ値を有することができる。コンピュータＩＤ値はポリシー１１３にプログラムすることができる。コンピュータ１２１～１２３のうちの識別されたコンピュータによってサーバ１１０に送信されるあらゆる印刷ジョブは、指定された保護レベル、最小保護レベル、および／または最大保護レベルを有することができる。ポリシー１１３は、印刷コマンドを入力したユーザおよび／または印刷ジョブを送信したコンピュータ１２１～１２３を識別することによって、印刷すべき文書１４０の保護要件を判定する。

【００１９】ポリシー１１３は、文書１４０の内容を探索して必要な保護レベルを判定することができる。この探索は、たとえば、文書１４０のキーワード探索またはキーフレーズ探索でよい。文書１４０の保護要件は、様々なキーワードまたはキーフレーズの発生回数に依存することができる。

【００２０】ポリシー１１３は、印刷すべき文書１４０のセキュリティ要件を決定する。たとえば、ポリシー１１３は、印刷すべき文書１４０に、標準的な複写機を使用したコピーによる偽造に対する保護が必要であることを決定することができる。あるいは、ポリシー１１３は、その走査、画像処理、および内容の変更に対する保

護が必要であることを決定することができる。ポリシー１１３がセキュリティ要件を決定した後、印刷管理システム１１２は、これらの要件を満たすのに必要な保護技法の特定の組合せを識別する。印刷管理システム１１２は次いで、信頼できるプリンタ１３１～１３５のうちの、適切な保護を適用できるプリンタに印刷ジョブを経路指定し、文書１４０に適切な保護技法が適用されるよ＊うに、選択されたプリンタにおけるパラメータを設定する。文書１４０を印刷する際に文書１４０に適用できる保護レベル、保護レベルの対象となる偽造技法、および保護レベルを生成し文書の真正さを検証するのに必要な機器の例について表１で説明する。

【００２１】

【表１】

保護レベル	技法	対象となる偽造技法	必要な機器
レベル０	脆弱な可変コピー証明透かし	標準的な複写機およびトナーまたはインクを有する偽造者。ブランクオリジナルアタック	標準的なカラープリンタ、あるいは特殊なトナーまたはインク、あるいはインスペクタを有する超高精細プリンタ
レベル１	追跡情報を有する頑強な可変不可視コピー証明透かし	コピー証明透かしをオリジナルから除去できる偽造者。ブランクオリジナルアタック。追跡を妨害するアタック	特殊なトナーまたはインクを有する標準カラープリンタ
レベル２	ページオフセットを印刷する蛍光性の脆弱な可変不可視コピー証明透かしと追跡情報	いたずらに対する弱い保護。ブランクオリジナルアタック	特殊なトナーまたはインクおよび標準的なハイライトプリンタまたはカラープリンタ。拡張機能として、トナーセンサまたはコピー証明透かしの存在を検証するセンサを含めることができる。検証のための蛍光灯
レベル３	ページオフセットを印刷する蛍光性の脆弱な可変不可視コピー証明透かしと、デジタル署名されグリフ符号化された追跡情報	走査、画像処理、および印刷を実行することができ、特殊なトナーまたはインクを得ることのできる偽造者	特殊なトナーまたはインクおよび標準的なハイライトプリンタまたはカラープリンタ。拡張機能として、トナーセンサまたはコピー証明透かしの存在を検証するセンサを含めることができる。検証のための蛍光灯および蛍光スキャナ。
レベル４	ページのランダム部分を印刷する蛍光性の脆弱な可変不可視コピー証明透かしと、デジタル署名されグリフ符号化された追跡情報	走査、画像処理、および印刷を実行することができ、特殊なトナーまたはインクを有する偽造者	特殊なトナーまたはインクおよび標準的なハイライトプリンタまたはカラープリンタ。拡張機能として、トナーセンサまたはコピー証明透かしの存在を検証するセンサを含めることができる。検証のための蛍光灯および蛍光スキャナ。
レベル５	追跡情報を有する、蛍光性の頑強な可変黒色コピー証明透かし	標準的な複写機およびトナーまたはインクを有する偽造者。追跡を妨害するアタック。	標準的なハイライトプリンタまたはカラープリンタにおける蛍光性黒色トナーまたはインク。検証のための蛍光灯
レベル６	蛍光性の頑強な可変黒色コピー証明透かしと、ページの一定の部分を印刷するための追跡情報	標準的な複写機およびトナーまたはインクを有する偽造者。トナーを除去するアタック。ブランクオリジナルアタック。	標準的なハイライトプリンタまたはカラープリンタにおける蛍光性黒色トナーまたはインク。検証のための蛍光灯
レベル７	ページのランダム部分を印刷する蛍光性の頑強な強い可変黒色コピー証明透かしと、暗号化されグリフ符号化されたランダムパターン記述	標準的な複写機およびトナーまたはインクを有する偽造者。スキャナおよび画像プロセッサを有する偽造者。トラーを除去するアタック。追跡を妨害するアタック。	標準的なハイライトプリンタまたはカラープリンタにおける蛍光性黒色トナーまたはインク。検証のための蛍光灯。グリフを読み取り検証するインスペクタ
レベル８	ページの内容依存部分を印刷する蛍光性の頑強な可変黒色コピー証明透かしと、暗号化されグリフ符号化された追跡情報	追跡情報を変更する偽造者。標準的な複写機およびトナーまたはインクを有する偽造者。走査および画像処理が可能な偽造者。トナーを除去するアタック。追跡を妨害するアタック。	標準的なハイライトプリンタまたはカラープリンタにおける蛍光性黒色トナーまたはインク。検証のための蛍光灯。グリフを読み取り検証するインスペクタ

【００２２】表１は、指定されたレベルの保護を文書に与えるために単独であるいは組み合わせて使用できる様々な透かし技法を示しているが、この表がポリシー１１３の１つの例示的な実施形態に過ぎないことを理解されたい。透かし技法の他の組合せによってより広い範囲の保護レベルを可能にすることができる。保護レベルと、各技法と、対象となる偽造方法と、印刷すべき文書に各技法を適用し、印刷される文書がオリジナルであるか、それとも偽造であるかを検証するのに必要な機器とについて以下に説明する。

【００２３】図１に示すように、信頼できるプリンタ１３１は、レベル０保護を持つ文書を印刷することができ、信頼できるプリンタ１３２は、レベル１保護が必要な文書を印刷することができ、信頼できるプリンタ１３３は、レベル０からレベル４の保護が必要な文書を印刷することができ、信頼できるプリンタ１３４は、レベル４からレベル８の保護が必要な文書を印刷することができ、信頼できるプリンタ１３５は、レベル７およびレベ

ル８の保護が必要な文書を印刷することができる。

【００２４】図２は、本発明による文書偽造防止印刷方法の１つの例示的な実施形態のフローチャートである。ステップＳ１０００から始まり、制御はステップＳ１１００に進み、ユーザが、偽造防止が必要な文書を作成する。次いで、ステップＳ１２００で、ユーザが、偽造防止が必要な文書を印刷するための印刷コマンドを入力する。次に、ステップＳ１３００で、保護レベルに関する情報がユーザに表示される。次いで、制御はステップＳ１４００に進む。

【００２５】ステップＳ１４００で、偽造防止が必要な文書の価値に関する情報が収集される。この情報には、偽造防止が必要な文書の潜在的な偽造と、様々な利用可能な保護技法を偽造防止が必要な文書に適用するコストとに関する情報または仮定を含めることができる。次に、ステップＳ１５００で、信頼できる印刷のポリシーに基づいて、偽造防止が必要な文書の保護要件が判定される。偽造防止が必要な文書の判定された保護要件は、この文書を、標準的な複写機を使用したコピーを防止する必要があるか、あるいは偽造防止を必要とする文書を、走査、画像処理、および文書の内容の変更を防止する必要があることを示すことができる。次いで、ステップＳ１６００で、判定された保護要件を満たす保護技法の特定の組合せを実現する保護レベルが判定される。次いで、制御はステップＳ１７００に進む。

【００２６】ステップ１７００で、偽造防止が必要な文書に適切な保護技法を適用できる信頼できるプリンタが、判定された保護レベルに基づいて選択される。次いで、ステップＳ１８００で、偽造防止が必要な文書の印刷ジョブが、選択された信頼できるプリンタに経路指定される。次に、ステップＳ１９００で、選択された信頼できるプリンタにおけるパラメータが、判定された保護レベルに基づいて設定される。ステップＳ２０００で、判定された保護レベルの保護技法を含め偽造防止が必要な文書が、選択された信頼できるプリンタを使用して印刷される。次いで、ステップＳ２１００で、この方法は終了する。

【００２７】上記に、本発明による文書偽造防止印刷方法の１つの例示的な実施形態について図２に関して説明したが、文書偽造防止保護印刷方法の他の例示的な実施形態が当業者には明らかであることを理解されたい。たとえば、本発明による文書偽造防止印刷方法の様々な例示的な実施形態では、印刷コマンドが入力される前に保護レベルに関する情報を表示することができる。本発明の文書偽造防止印刷方法の発明の他の様々な例示的な実施形態では、印刷コマンドが入力される前に、文書の価値および文書の潜在的な偽造に関する情報を収集することもできる。本発明による文書偽造防止印刷方法の他の様々な例示的な実施形態では、印刷ジョブが、選択された信頼できるプリンタに経路指定される前に、選択された信頼できるプリンタのパラメータを設定することができる。

【００２８】図１に示すように、信頼できるプリンタ１３１および１３３は、レベル０保護を有する文書を印刷することができる。表１に示すように、レベル０保護には材弱な可変コピー証明透かしが含まれる。図３に示すように、内容所有者、たとえば、文書１４０を作成し、文書１４０を見て、かつ／または文書１４０を印刷することを許可された人は、画像データ供給源、たとえば、コンピュータ１２１～１２３のうちの１つまたは外部データ記憶装置からの画像データを画像プロセッサに供給する。

【００２９】コピーの証拠も画像プロセッサに供給され、文書１４０の内容に含められる。文書１４０に含められるコピーの証拠は、文書１４０のページごとに異なる証拠でよく、ページの内容、ページ番号または識別子、著者、文書タイトル、日付、時間、および発生元組織を識別する情報を含むことができる。コピーの証拠には、信頼できるプリンタ１３１または１３３に関する特性、あるいは信頼できるプリンタ１３１または１３３によって記録される固有のコピー番号を含めることもできる。コピーの証拠は、それぞれのコンピュータ１２１～１２３の表示ユニット１５１～１５３のうちの１つに設けられたグラフィカルユーザインタフェースを通して内容所有者によって供給するか、あるいはオペレーティングシステム１１１、印刷管理システム１１２、および／またはポリシー１１３によって自動的に決定することができる。コピーの証拠は、脆弱な可変コピー証明透かしとして符号化される。コピーの証拠が文書の各ページごとに異なるので、脆弱な可変コピー証明透かしは各ページごとに異なる。

【００３０】レベル０の脆弱な可変コピー証拠透かしは、脆弱な透かしを形成する任意の公知の技法によって形成することができる。脆弱な透かしを形成する技法には、たとえば、文字内でのインク密度の微小変動、文字に含まれる極端に小さなグリフ、文書が印刷される記録材料のシートの背景あるいは１つまたは複数の未使用部分に印刷され、当該シートにおける陰影または繊維として表示される、場合によってはカラーの非常に小さなマークまたはテクスチャ、テキストの文字内の超高精細画素、カラー画像または白黒画像内のサーペントン(serpentone)が含まれる。

【００３１】印刷すべき文書１４０のセキュリティ要件に脆弱な可変コピー証明透かしが必要であることがポリシー１１３によって決定されている場合、印刷管理システム１１２は印刷ジョブを信頼できるプリンタ１３１または１３３に経路指定する。印刷管理システム１１２はまた、信頼できるプリンタ１３１または１３３におけるパラメータを、脆弱な可変コピー証明透かしを印刷するように設定する。

【００３２】脆弱な可変コピー証明透かしは、信頼できるプリンタ１３１または１３３に含まれるか、あるいは内容所有者に属する秘密鍵によってのみ情報を復号できるように、脆弱な可変コピー証明透かしにコピーの証拠を符号化することによって、脆弱な可変コピー証明透かしの偽造をより困難にすることができる。脆弱な可変コピー証明透かしに含まれるコピーの証拠は、信頼できるプリンタ１３１または１３３の固有の物理的特性に依存することもできる。たとえば、引用によって本明細書に全体的に組み込まれている米国特許出願第０９／５０４０３６号に開示されたように信頼できるプリンタ１３１または１３３によって文書にランダムパターンを適用することができる。偽造者といった敵に知られていないコピーの証拠を脆弱な可変コピー証明透かしに符号化することもできるし、あるいは、脆弱な可変コピー証明透かしを、例えば分光変調など再現するのが困難であるか、あるいは再現するのに費用がかかる方法を使用して印刷することができる。

【００３３】表１に示すように、信頼できるプリンタ１３１または１３３は、たとえば、蛍光性や磁性を有するトナーやインクなど、特殊なトナーまたはインクを供給される標準的なカラープリンタまたは標準的なプリンタでよい。信頼できるプリンタ１３１または１３３は、サーペントンを印刷できる超高精細プリンタでもよい。インスペクタ装置を使用して、サーペントンの存在あるいは特殊なトナーまたはインクの存在を検証することができる。インスペクタ装置は、脆弱な可変コピー証明透かしの内容を読み取ることもできる。このようなプリンタおよびインスペクタ装置は、それぞれ引用によって本明細書に全体的に組み込まれている米国特許第５７０６０９９号および米国特許第５７１０６３６号に開示されている。

【００３４】図３に示すように、信頼できるプリンタ１３１または１３３は文書１４０を標準紙上に印刷する。標準紙とは、事前に印刷された透かしを必ずしも有さない紙である。図３に示すように、レベル０の脆弱な可変コピー証明透かしが印刷された文書１４０は、偽造者がこのオリジナル印刷文書と標準的なトナーまたはインクを有する標準的な複写機とを使用することを妨げる。視覚的インスペクタは、文書がオリジナルであるか、それとも偽造であるかを検証することができる。視覚的インスペクタは、文書が真正であるかどうかを検査することが許可された人であってよい。文書は、脆弱な可変コピー証明透かしの外観が歪められていないことによってオリジナルとして検証される。文書は、脆弱な可変コピー証明透かしがないこと、あるいは脆弱な可変コピー証明透かしが変色していることによって偽造とみなされる。コピー証明透かしを生成するために使用される技法に応じて、コピー証明透かしの存在を検証し、コピー証明透かしの内容を読み取るためにインスペクタ装置が必要である。

【００３５】図３に示すように、レベル０の脆弱な可変コピー証明透かしのコピーの証拠が、印刷されるページと共に変化するので、レベル０はブランクオリジナルアタックに対する保護も行う。ブランクオリジナルアタックとは、ブランクオリジナル上にオリジナル文書をコピーすることによって偽造を試みることである。ブランクオリジナル、すなわち白紙オリジナルとは、事前に印刷された脆弱な透かしを含む記録材料のシートである。しかし、ブランクオリジナルの事前に印刷された脆弱な透かしは、印刷されるページごとに異なるものではない。したがって、事前に印刷された不変の脆弱な透かしの存在を視覚的インスペクタによって検出することができる。不変の脆弱な透かしを検出することによって文書は偽造とみなされる。

【００３６】図１に示すように、信頼できるプリンタ１３２または１３３はレベル１保護を有する文書を印刷することができる。表１に示すように、レベル１保護は、追跡情報を有する頑強な不可視可変コピー証明透かしを含む。頑強な不可視可変コピー証明透かしは、頑強な透かしを形成するための任意の公知の技法または後で開発される技法によって形成することができる。頑強な透かしを形成する技法には、たとえば、基線に対する文字のわずかな垂直並進、文字間の間隔のわずかな変化、行インデント、マージン、および／または行間隔が含まれる。頑強な透かしは、輝度パターンまたはグレースケールノイズ状パターンを付加することによって形成することもできる。

【００３７】レベル１の頑強な不可視可変コピー証明透かしを使用してコピーの証拠および追跡情報を符号化することができる。文書１４０に含められるコピーの証拠は、文書１４０のページごとに異なる証拠でよく、ページの内容、ページ番号または識別子、著者、文書タイトル、日付、時間、および発生元組織を識別する情報を含むことができる。コピーの証拠には、信頼できるプリンタ１３１または１３３に関する特性、あるいは信頼できるプリンタ１３１または１３３によって記録される固有のコピー番号を含めることもできる。コピーの証拠は、たとえば「これはコピーです」やある種の同様な警告など、警告文を目立つように表示する大きなバナーを含むこともできる。追跡情報には、たとえば、オリジナル文書が誰に与えられた文書であるか、この文書を所有することを許可されているのは誰かを識別する情報、およびコピー制限または文書中の情報の使用に関するその他の制限に関する情報を含めることができる。追跡情報は、データ所有権言語で指定することができる。コピーの証拠および追跡情報は、頑強な不可視可変コピー証明透かしに符号化される。

【００３８】図４に示すように、内容所有者は、画像データ供給源、たとえば、コンピュータ１２１～１２３の

うちの１つや外部データ記憶装置からの画像データを、画像プロセッサ、たとえば、サーバ１１０上に記憶されているアプリケーションに供給し、文書を作成する。コピーの証拠および追跡情報は、画像プロセッサにも供給され、文書１４０の内容に含められる。コピーの証拠および追跡情報は、文書１４０の画像処理中に、文書１４０の内容に含められる。文書１４０に含められたコピーの証拠および追跡情報は、それぞれのコンピュータ１２１～１２３の表示ユニット１５１～１５３のうちの１つに設けられたグラフィカルユーザインタフェースを通して内容所有者によって入力するか、あるいはオペレーティングシステム１１１、印刷管理システム１１２、および／またはポリシー１１３によって自動的に決定することができる。

【００３９】印刷管理システム１１２は、印刷ジョブを信頼できるプリンタ１３２または１３３に経路指定し、文書は標準紙上に印刷される。図４に示すように、レベル１では、このオリジナル文書１４０と、標準的な複写機ならびに標準的な用紙およびトナーまたはインクとを得ることのできる偽造者に対する防御が実現される。偽造者が標準的なトナーまたはインクと標準紙とを使用して標準的な複写機上でオリジナル文書１４０をコピーした場合、視覚的インスペクタは、結果として得られるコピー上の頑強な可変コピー証明透かしのはっきりと見える外観に注目することによって、結果として得られるコピーを偽造とみなすことができる。文書に頑強な可変コピー証明透かしがないようである場合、このことは、この文書はオリジナルであるが、第２段階の検査が必要であることを示している。

【００４０】図４に示すように、第２段階の検査では、文書がオリジナルであるかどうかを判定することができる。文書は標準紙を使用して標準的な複写機上でコピーされる。結果として得られるコピーがはっきりと見える透かしを含んでいる場合、このオリジナル文書をオリジナルとして検証することができる。

【００４１】表１に示すように、レベル１では、たとえば、文書を走査し、画像処理時に透かしを除去または削除することによって、頑強な可変コピー証明透かしを除去することのできる偽造者に対する防御が実現される。表１および図４に示すように、レベル１では、ブランクオリジナルアタックも防止される。レベル１では、偽造者が追跡情報源を妨害するか、あるいは追跡情報源にいたずらする、追跡を妨害するアタックも防止される。信頼できるプリンタ１３２または１３３は、たとえば蛍光トナーまたは蛍光インクを含む特殊なトナーまたはインクを使用することのできる標準的なカラープリンタでよい。

【００４２】図１に示すように、信頼できるプリンタ１３３は、レベル２保護を有する文書を印刷することができる。表１に示すように、レベル２保護は、追跡情報を有する蛍光性の脆弱な可変不可視コピー証明透かしを含む。コピーの証拠は、ある距離だけずれたページのテキストを含むことができるが、いずれの場合もページの内容に依存する。コピーの証拠および追跡情報は、蛍光性の脆弱な可変不可視コピー証明透かしに符号化することができる。図５に示すように、内容、コピーの証拠、および追跡情報を含む文書は、信頼できるプリンタ１３３により特殊なトナーまたはインクを使用して標準紙上に印刷される。特殊なトナーまたはインクは蛍光性で不可視のトナーまたはインクである。表１に示すように、信頼できるプリンタ１３３は、蛍光不可視のトナーまたはインクを備える標準的なハイライトプリンタまたはカラープリンタでよい。プリンタの出力上のセンサは、コピー証明マークが適切に印刷されたことを検証することができる。

【００４３】コピー証明マークの可変性により、偽造者が用紙に特殊なマークを付けることによって用紙を前処理するブランクオリジナルアタックが防止される。識別情報により、許可されていないコピー動作の源を追跡することもできる。すなわち、基礎的な情報により、オリジナルの管理権を有しており、オリジナルを保護していたであろう人は誰かが識別される。ページ上の２つの印刷が蛍光の下では視覚的に異なるので、文書の内容のいたずらを試みる偽造者に対するある種の防御を実現するためにレベル２保護を使用することができる。

【００４４】表１および図５に示すように、レベル２では、オリジナル文書と標準的なトナーまたはインクを有する標準的な複写機とを得ることのできる偽造者に対する防御が実現される。文書は、それを蛍光励起光で照明することによってオリジナルとして検証することができる。文書が、透かしを有さないか、蛍光励起光の下で蛍光を発しない透かしを有するか、あるいは蛍光を発するが、そのページの可視内容と一致しない透かしを含んでいる場合、その文書をコピーとみなすことができる。

【００４５】図１に示すように、信頼できるプリンタ１３３は、レベル３保護を有する文書を印刷することができる。表１に示すように、レベル３保護は、追跡情報を有する蛍光性の脆弱な可変不可視コピー証明透かしを含む。この透かしは、ある距離だけずらされ不可視蛍光トナーを使用して印刷されたページのテキストのコピーまたは一部を含む。プリンタ、ユーザ、タイムスタンプ、文書ＩＤ、ページ番号などの追跡情報も不可視インクを使用して印刷される。コピー証明マークに含まれている情報は、デジタルに署名され、ページの左マージンに印刷されるグリフ符号として符号化される。

【００４６】表１および図６に示すように、レベル３では、走査、画像処理、および印刷を行うことができ、したがって、文書の内容へのいたずらを試み、使用される特殊なインクを得ることのできる偽造者に対する防御が実現される。単純な偽造者に対する防御は、レベル２保

護と同様に蛍光検出器を介して行われる。追加的ないたずら防止および真正さは、グリフ符号として符号化されたデジタル署名によって実現される。

【００４７】特殊なインクおよび通常のハイライトプリンタまたは通常のカラープリンタを使用してオリジナル文書を印刷することができる。プリンタの拡張機能として、蛍光トナーが装填され使用されていることを検査するセンサを含めることができる。また、プリンタの出力上のセンサを使用して、コピー証明透かしが適切に印刷されていることを検証することができる。蛍光励起光源を使用してコピー証明透かしを露光し、蛍光スキャナを使用して、蛍光インクで印刷された情報を読み取ることができる。この方法は、レベル２保護と後方互換性を有する。

【００４８】図６に示すように、文書は、ページの可視内容と一致する蛍光コピー証明透かしが存在すること、またはグリフ符号として符号化されたデジタル署名の検証が成功することによってオリジナルとして検証することができる。文書は、蛍光コピー証明マークが存在しないことによってコピーとして検証することができる。蛍光コピー証明透かしが存在する場合、デジタル署名が首尾良く検証できない場合には、その文書を依然としてコピーとして検証することができる。

【００４９】図１に示すように、信頼できるプリンタ１３３および１３４は、レベル４保護を有する文書を印刷することができる。表１に示すように、レベル４保護は、ランダムに生成されるパターンを印刷する蛍光性の脆弱な不可視可変コピー証明透かしを含む。このコピー証明透かしには追跡情報も含められる。コピー証明透かしのランダムパターンは、デジタルに署名され、ページ上に印刷されるグリフ符号として符号化される。

【００５０】図７に示すように、レベル４では、スキャナ、画像処理ソフトウェア、およびカラープリンタを使用できると共に、使用される特殊なインクを得ることができ、これらを使用して文書に内容にいたずらするか、あるいは許容されるコピー証明マークの偽造を試みる偽造者に対する防御が実現される。追加的ないたずら防止および真正さは、グリフ符号として符号化されたデジタル署名によって実現される。

【００５１】特殊なインクおよび通常のハイライトプリンタまたは通常のカラープリンタを使用してオリジナル文書を印刷することができる。プリンタの拡張機能として、蛍光トナーが装填され使用されていることを検査するセンサを含めることができる。また、プリンタの出力上のセンサを使用して、コピー証明透かしが適切に印刷されていることを検証することができる。蛍光励起光源を使用してコピー証明透かしを露光することができる。蛍光励起光スキャナを使用して、蛍光インクで印刷された情報を読み取ることができる。

【００５２】図７に示すように、文書は、用紙から測定された蛍光パターンが、グリフ符号として符号化されたパターンと一致するか、あるいはデジタル署名の検証が成功することによってオリジナルとして検証することができる。文書は、蛍光コピー証明マークが存在しないことによってコピーとして検証することができる。コピー証明透かしが存在する場合、用紙から測定された蛍光パターンが、グリフ符号として符号化されたパターンと一致しない場合には、その文書を依然としてコピーとして検証することができる。

【００５３】図１に示すように、信頼できるプリンタ１３４は、レベル５保護を有する文書を印刷することができる。表１に示すように、蛍光性の頑強な黒色コピー証明透かしを使用することによってコピーの証拠が与えられる。この透かしには追跡情報が符号化される。図８に示すように、レベル５では、標準的な複写機を使用して許可されていないコピーを行うか、あるいは偽造を試み、かつ蛍光インクを得ることができない偽造者に対する防御が実現される。レベル５保護を可能にするために使用できる機器は、通常のハイライトプリンタまたはカラープリンタにおける蛍光黒色トナーである。蛍光励起光源は、コピー証明透かしの検証を助けることができる。

【００５４】文書は、それを視覚的に検査することによってオリジナルとして検証することができる。視覚検査によって蛍光黒色コピー証明マークを見つけることができる。文書は、コピー証明透かしが存在しないこと、または通常のインクで印刷されたコピー証明透かしによってコピーとして検証することができる。

【００５５】図１に示すように、信頼できるプリンタ１３４は、レベル６保護を有する文書を印刷することができる。表１に示すように、蛍光性の頑強な黒色コピー証明透かしを使用することによってコピーの証拠が与えられる。たとえば、このような透かしは、通常の黒色インク上に蛍光不可視インクを印刷することによって作成することができる。蛍光黒色インクを使用して、文書内容の一定の部分が印刷される（このように印刷される部分として選択される部分は、文書内容に依存しない）。この透かしには追跡情報を符号化することもできる。図９に示すように、レベル６では、通常の複写機を使用して許可されていないコピーを行うか、あるいは偽造を試み、かつこの特殊なインクを得ることができない偽造者に対する防御が実現される。レベル６では、蛍光トナーを除去する信頼できるプリンタに物理的にアクセスできる偽造者に対する防御も実現される。これは、蛍光トナーを除去すると、印刷されたページの一部が消えてしまうからである。

【００５６】レベル６保護を実現するために使用できる機器には、通常のハイライトプリンタまたはカラープリンタにおける蛍光黒色トナー、または蛍光不可視インクと通常の黒色インクとの組合せが含まれる。特殊なビュ

ーアを使用して、コピー証明透かしの正しいパターンを検出し検証することができる。

【００５７】図９に示すように、文書は、それを視覚的に検査して、文書ページの内容全体が印刷されていることを検証することによって、オリジナルとして検証することができる。特殊なビューアを使用して、文書の可視内容の一部が蛍光を発していることを検証するか、あるいは正しい蛍光パターンを検証することができる。文書は、それを視覚的に検査することによってコピーとして検証することができる。ページの一部が印刷されていない場合、その文書をコピーとして検証することができる。ページ全体が印刷されている場合、蛍光黒色コピー証明透かしが存在しないか、あるいは非蛍光コピー証明マークが存在することによって、その文書をコピーとして検証することができる。文書は、特殊なビューアにより、コピー証明マーク中の蛍光パターンが正しくないことが判明した場合に、コピーとして検証することができる。

【００５８】図１に示すように、信頼できるプリンタ１３４または１３５は、レベル７保護を有する文書を印刷することができる。表１に示すように、レベル７保護は、蛍光性の頑強な黒色可変コピー証明透かしを含む。図１０に示すように、蛍光黒色トナーまたはインクを使用することにより、文書の内容のランダムに選択された部分が印刷される。どのパターンが使用されているかに関する情報は、信頼できるプリンタ１３４および１３５ならびにインスペクタ装置に知られている鍵を使用して文書上に印刷されるグリフ符号として暗号化され符号化される。インスペクタ装置は、グリフ符号を読み取り、グリフ符号を復号して暗号化パターンを得て、パターン情報を復号することができる。この透かしにはコピーの証拠および追跡情報も符号化される。

【００５９】図１０に示すように、レベル７では、オリジナル文書および信頼できるプリンタ１３４または１３５を使用することができるが、蛍光黒色トナーまたはインクを得ることのできない偽造者に対する防御が実現される。レベル７では、蛍光トナーを除去する信頼できるプリンタに物理的にアクセスできる偽造者に対する防御も実現される。これは、蛍光トナーを除去すると、印刷されたページの一部が消えてしまうからである。レベル７では、スキャナおよび画像プロセッサを有する偽造者に対する防御も実現される。

【００６０】文書がオリジナルであることの検証は、蛍光励起光を使用して行うことができる。蛍光励起光にさらされたときに文書の一部が蛍光を発した場合、このことは、この文書がオリジナルではないことを示す。この場合、第２段階の検査が必要である。インスペクタ装置は、復号されたグリフ符号化情報が蛍光パターンに整合することを検証する。文書の一部が欠落している場合、その文書をコピーとして検証することができる。文書全体が印刷されているが、透かしがないか、あるいは蛍光を発しない黒色透かしが存在する場合、その文書をコピーとみなすことができる。文書が蛍光部分を有するが、復号されたグリフ符号化情報が蛍光パターンに整合しない場合、その文書をコピーとみなすことができる。復号されたパターン情報が、検出されたパターンに整合する場合、その文書をオリジナルとして検証することができる。

【００６１】信頼できるプリンタ１３４および１３５は、蛍光黒色トナーを備える標準的なハイライトプリンタまたはカラープリンタでよい。図１に示すように、信頼できるプリンタ１３４および１３５は、レベル８保護を有する文書を印刷することができる。表１に示すように、レベル８保護は、文書の内容依存部分を印刷する蛍光性の頑強な黒色可変コピー証明透かしと、プリンタおよびインスペクタ装置に知られている鍵によって暗号化されグリフ符号化された追跡情報とを含む。この透かしは、蛍光黒色トナーまたはインクで印刷される文書の内容の選択された部分を含む。この選択された部分は、文書の内容の関数として選択される。ユーザおよび信頼できるプリンタ１３４または１３５に関する情報と蛍光パターンとが暗号化され、文書上に印刷されるグリフ符号として符号化される。

【００６２】表１に示すように、レベル８では、オリジナル文書と標準的な複写機およびトナーまたはインクを得ることのできる偽造者に対する防御が実現される。図１１に示すように、レベル８では、オリジナル文書、スキャナ、画像プロセッサ、および信頼できるプリンタ１３４または１３５を得ることができ、追跡情報の変更を試みる偽造者に対する防御も実現される。偽造者が追跡情報の変更を試みた場合でも、偽造者には追跡情報を暗号化または復号するための鍵がわからない。レベル８では、トナーを除去するアタックも防止される。これは、蛍光トナーを除去すると、印刷されたページの一部が消えてしまうからである。

【００６３】文書をコピーとみなすことは、視覚検査によって行うこともできる。印刷された文書の一部が欠落している場合、その文書をコピーとみなすことができる。文書全体が印刷されているが、透かしがないか、あるいは蛍光を発しない黒色透かしが存在する場合、その文書をコピーとみなすことができる。インスペクタ装置によってグリフ符合から復号されたパターン情報が、蛍光スキャナによって検出された蛍光パターンと一致するかどうかが第２段階の検査によって判定される。復号されたパターン情報が、検出されたパターンに整合する場合、その文書をオリジナルとして検証することができる。

【００６４】信頼できるプリンタ１３４および１３５は、蛍光黒色トナーを備える標準的なハイライトプリンタまたはカラープリンタでよい。蛍光スキャナを使用し

17

て蛍光パターンを検出することができ、インスペクタ装置を使用してグリフを読み取り、グリフを復号して暗号化されたパターン情報を得て、パターン情報を復号し、パターン情報を検出された蛍光パターンと突き合わせることができる。

【図面の簡単な説明】

【図１】　本発明による印刷管理システムを示す概略図である。

【図２】　本発明の例示的な実施形態による文書偽造防止印刷方法のフローチャートである。

【図３】　本発明の例示的な実施形態による文書偽造防止印刷・検出システムの流れ図である。

【図４】　本発明の例示的な実施形態による文書偽造防止印刷・検出システムの流れ図である。

【図５】　本発明の例示的な実施形態による文書偽造防止印刷・検出システムの流れ図である。

【図６】　本発明の例示的な実施形態による文書偽造防止印刷・検出システムの流れ図である。

18

＊【図７】　本発明の例示的な実施形態による文書偽造防止印刷・検出システムの流れ図である。

【図８】　本発明の例示的な実施形態による文書偽造防止印刷・検出システムの流れ図である。

【図９】　本発明の例示的な実施形態による文書偽造防止印刷・検出システムの流れ図である。

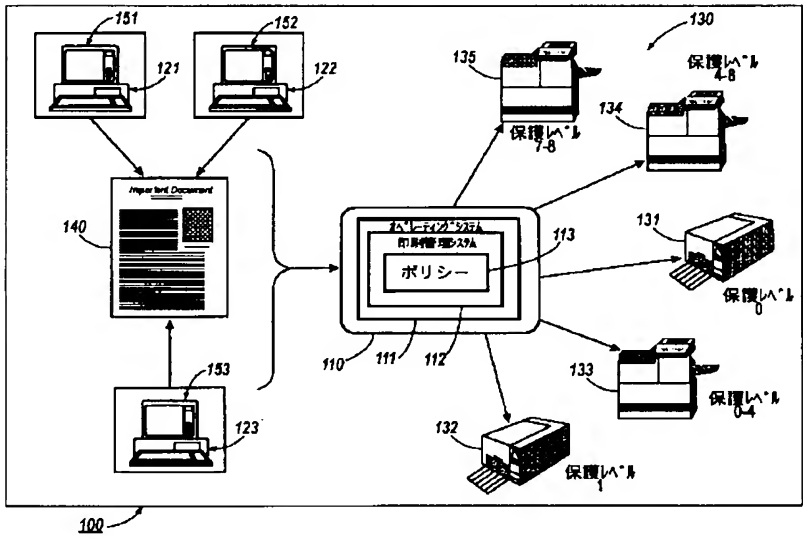
【図１０】　本発明の例示的な実施形態による文書偽造防止印刷・検出システムの流れ図である。

【図１１】　本発明の例示的な実施形態による文書偽造防止印刷・検出システムの流れ図である。

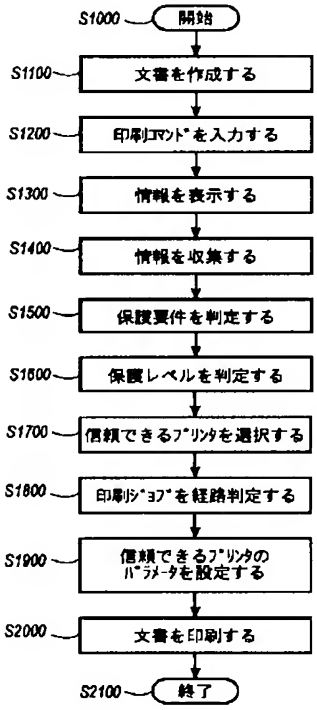
【符号の説明】

１００　ネットワーク、１１０　サーバ、１１１　オペレーティングシステム、１１２　印刷管理システム、１１３　ポリシー、１２１，１２２，１２３　コンピュータ、１３１，１３２，１３３，１３４，１３５　プリンタ、１４０　文書、１５１，１５２，１５３　表示ユニット。

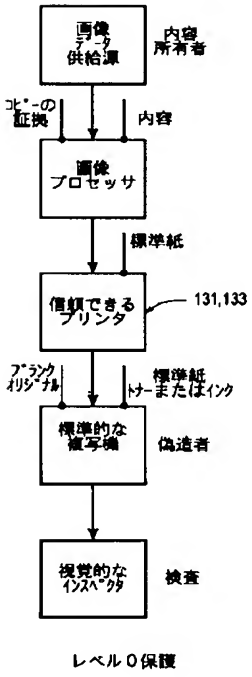
【図１】



【図２】

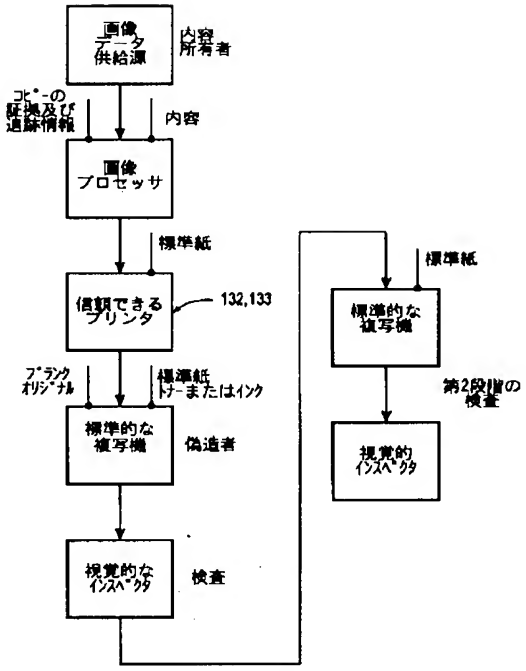


【図３】



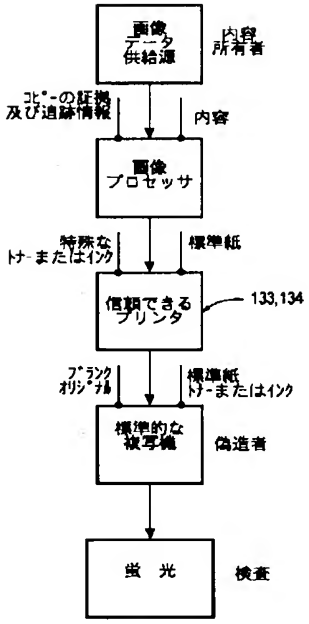
レベル０保護

【図４】



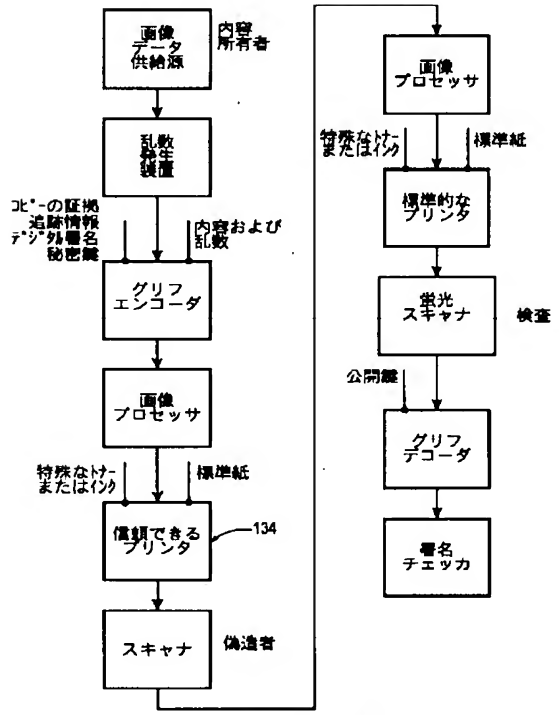
レベル１保護

【図５】



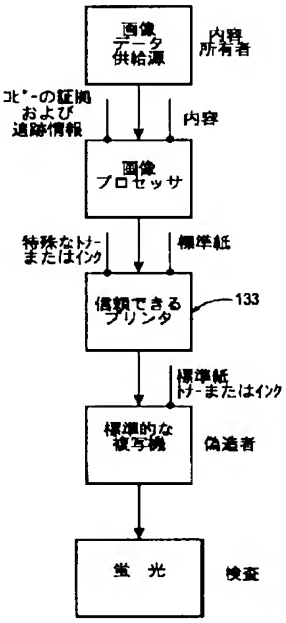
レベル２保護

【図７】



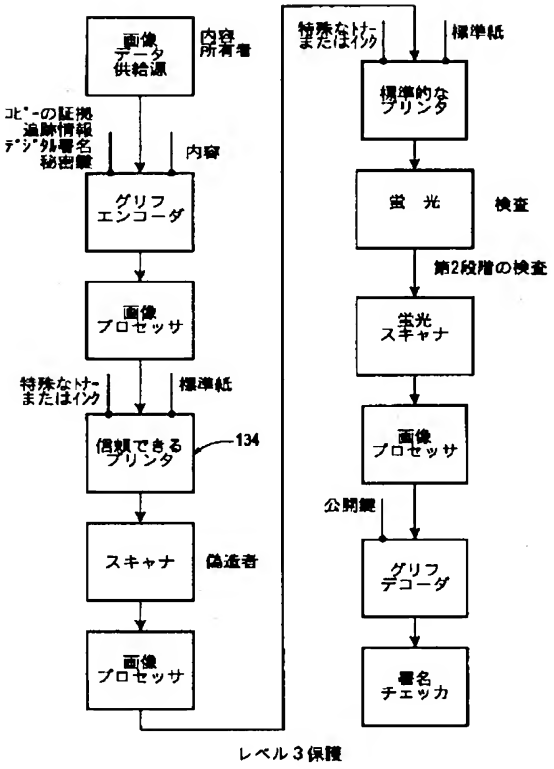
レベル４保護

【図８】

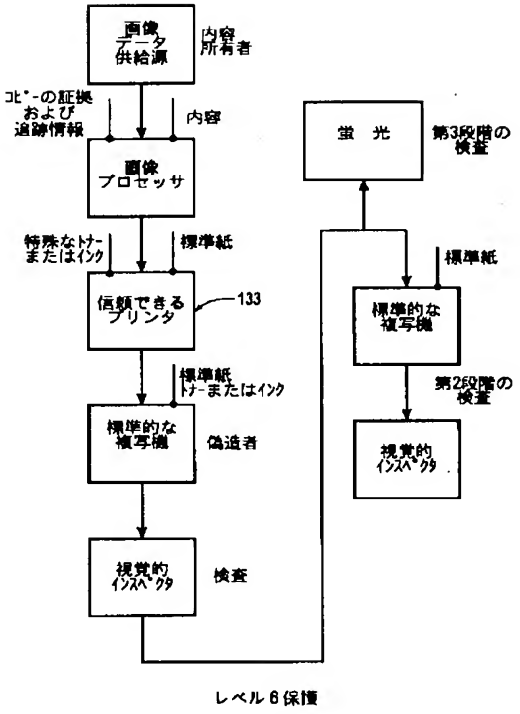


レベル５保護

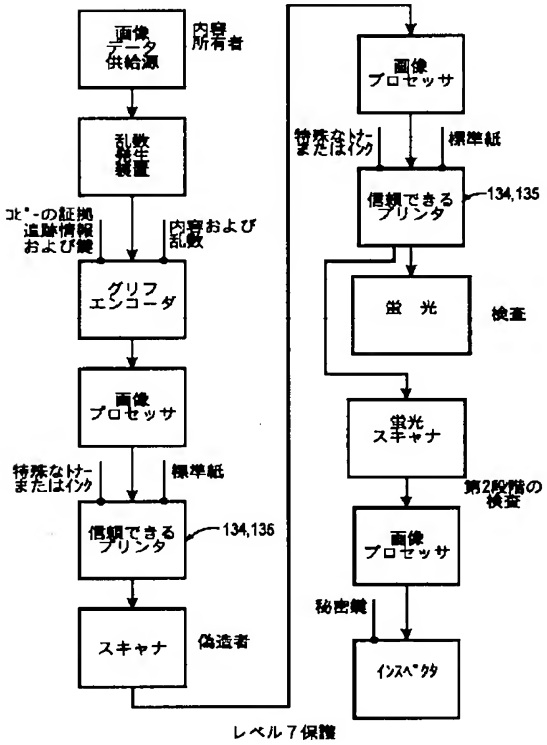
【図６】


画像データ供給源
内容所有者
ｺﾋﾟｰの証拠
追跡情報
ﾃﾞｼﾞﾀﾙ署名
秘密鍵
内容
グリフエンコーダ
画像プロセッサ
特殊なﾄﾅｰまたはｲﾝｸ
標準紙
信頼できるプリンタ
134
スキャナ
偽造者
画像プロセッサ
特殊なﾄﾅｰまたはｲﾝｸ
標準紙
標準的なプリンタ
蛍光
検査
第2段階の検査
蛍光スキャナ
画像プロセッサ
公開鍵
グリフデコーダ
署名チェッカ
レベル３保護

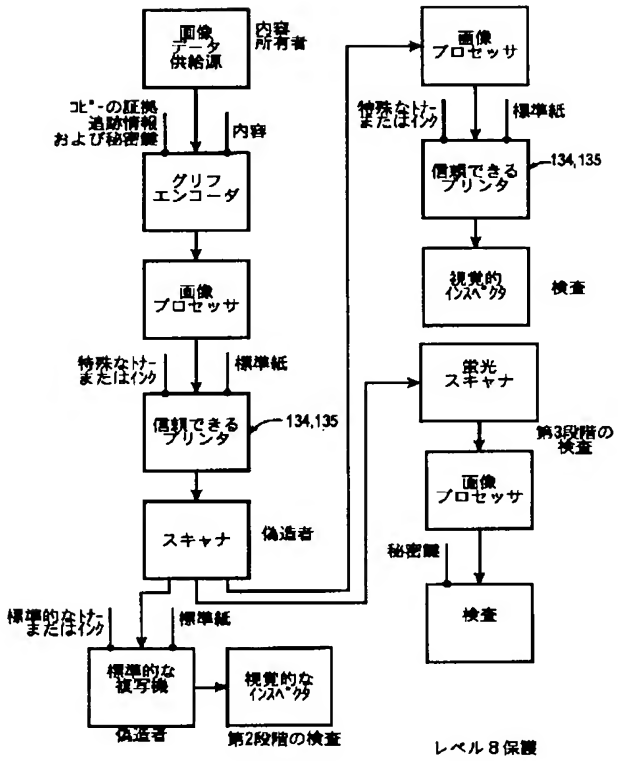
【図９】


画像データ供給源
内容所有者
ｺﾋﾟｰの証拠
および
追跡情報
内容
画像プロセッサ
特殊なﾄﾅｰまたはｲﾝｸ
標準紙
信頼できるプリンタ
133
標準紙
ﾄﾅｰまたはｲﾝｸ
標準的な複写機
偽造者
視覚的ｲﾝｽﾍﾟｸﾀ
検査
蛍光
第3段階の検査
標準紙
標準的な複写機
第2段階の検査
視覚的ｲﾝｽﾍﾟｸﾀ
レベル６保護

【図１０】


画像データ供給源
内容所有者
乱数発生装置
ｺﾋﾟｰの証拠
追跡情報
および鍵
内容および乱数
グリフエンコーダ
画像プロセッサ
特殊なﾄﾅｰまたはｲﾝｸ
標準紙
信頼できるプリンタ
134,135
スキャナ
偽造者
画像プロセッサ
特殊なﾄﾅｰまたはｲﾝｸ
標準紙
信頼できるプリンタ
134,135
蛍光
検査
蛍光スキャナ
第2段階の検査
画像プロセッサ
秘密鍵
ｲﾝｽﾍﾟｸﾀ
レベル７保護

【図１１】



フロントページの続き

(51)Int.Cl.⁷	識別記号	FI	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｔ　1/00	５００	Ｂ４１Ｊ　29/00	Ｚ　５Ｃ０７７
Ｈ０４Ｎ　1/40		Ｈ０４Ｎ　1/40	Ｚ

(72)発明者　デビッド　エル　ヘクト
アメリカ合衆国　カリフォルニア州　パロ　アルト　バーバラ　ドライブ　2001
(72)発明者　トーマス　エー　バーソン
アメリカ合衆国　カリフォルニア州　パロ　アルト　フォレスト　アベニュー　764
(72)発明者　マーク　ジェー　ステフィク
アメリカ合衆国　カリフォルニア州　ウッドサイド　ビッグ　ツリー　ウェイ　55
(72)発明者　アール　ドリュース　ディーン
アメリカ合衆国　カリフォルニア州　クパーチノ　ホワイト　ファー　コート　21070
(72)発明者　アラン　ジー　ベル
アメリカ合衆国　カリフォルニア州　パロ　アルト　エメルソン　ストリート　2125
(72)発明者　トーマス　エム　ブリュエル
アメリカ合衆国　カリフォルニア州　サン　ホセ　サウス　４ティーエイチ　ストリート　201　＃542
(72)発明者　トッド　エー　カス
アメリカ合衆国　カリフォルニア州　サン　フランシスコ　ディグビー　ストリート　4
(72)発明者　ダグラス　エヌ　カリー
アメリカ合衆国　カリフォルニア州　メンロー　パーク　ルランド　アベニュー　221
(72)発明者　ダニエル　エイチ　グリーン
アメリカ合衆国　カリフォルニア州　サニーベール　マネット　ドライブ　1055　＃６

(72)発明者　ロバート　ティー　クリバシク
アメリカ合衆国　カリフォルニア州　サン
ホセ　ガンナー　ドライブ　2302

Ｆターム(参考)　2C061 AP04 AQ05 AQ06 AS02 CL08
CL10 HK03 HQ14
2C087 AA09 AA13 AB06 AB08 AC07
AC08 CA05 DA14
5B021 AA01 LD15 NN00 NN16
5B057 AA11 CB19 CE08
5C076 AA14 BA06
5C077 LL14 PP23 TT02 TT06